



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,394	02/06/2004	Shehzad T. Merchant	02453.0020.NPUS00	6341
27194 7590 02/20/2007 HOWREY LLP C/O IP DOCKETING DEPARTMENT 2941 FAIRVIEW PARK DRIVE, SUITE 200 FALLS CHURCH, VA 22042-2924			EXAMINER AHUJA, SUPRIYA	
			ART UNIT	PAPER NUMBER
			2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/773,394

Applicant(s)

MERCHANT ET AL.

Examiner

Supriya Ahuja

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 February 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: ____.

DETAILED ACTION.

Drawings

1. The drawings are objected to under 37 CFR 1.83(a) because they fail to show network system 10 and network 11 in Figure 2 as described in the specification on page 6, lines 22 and 25. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character “154” has been used to designate both store sensitive information in network and attach network device in the block diagram of Figure 1. Corrected drawing

Art Unit: 2109

sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities:

This application is informal in the arrangement of the specification because the specification includes a list of the names of the inventors on page 1 of the specification, which should be deleted from the specification.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.

Art Unit: 2109

- (e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
- (f) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (g) BRIEF SUMMARY OF THE INVENTION.
- (h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (i) DETAILED DESCRIPTION OF THE INVENTION.
- (j) CLAIM OR CLAIMS (commencing on a separate sheet).
- (k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

On page 1, line 17 and 19 of the specification, the phrase "To Be Determined" should be replaced by the appropriate application no.

On page 6, line 10 of the specification, the acronym "POE" should be replaced by --PoE--.

On page 12, line 19 of the specification, the phrase "the goes" should be replaced by --that goes--.

Appropriate correction is required.

Claim Objections

4. **Claims 1-3,8-10,22,26,32** are objected to because of the following informalities:

In claims 1 and 8, line 8, the phrase "that device" should be replaced by --that the device--.

Art Unit: 2109

In claims 2-3 and 9-10, line 2, the phrase "the group" lacks antecedent basis and should be replaced by --a group--.

In claim 22, line 2, the phrase "the network" lacks antecedent basis and should be replaced by --a network--.

In claim 26, line 3, the phrase "the wireless AP" lacks antecedent basis and should be replaced by --a wireless AP--.

In claim 32, line 2, the phrase "security information" should be replaced by --the security information--.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1, 5,8,12** are rejected under 35 U.S.C. 102(b) as being anticipated by Beckmann (5,659,604 dated 08/19/1997).

Claim 1. A system (system, see abstract line 1, col.3 line 32) for protecting sensitive information (call records, col. 3, line 38) in a network (local area network (LAN), col. 3 line 33), comprising: a network component (switch, abstract line 4) for storing (abstract lines 4-5) the sensitive information; and a network device (adjunct processor (AP), abstract line 4, col.3 lines 2-3), attachable to the network, that lacks the sensitive information and is inoperative, at least in part, until the sensitive information is stored

therein; wherein when the network device is attached to the network, the sensitive information is downloaded (col. 3 line 39) from the network component and stored in the network device so that device becomes operational; wherein when the network device is disconnected from the network, the sensitive information is erased from the network device, whereby making the device inoperative at least in part and removing the sensitive information from the device (According to hyperdictionary online: volatile storage is a computer storage that is erased when the power is turned off. Therefore, it is factual in nature that if the power is disconnected from the device, the volatile memory (RAM) of the device would lose any data as soon as it is disconnected and the device will be non-operational).

Claims 5 and 12. Beckmann discloses all the limitations of claim 5. The network component is a LAN switch (switch, abstract line 4).

Claim 8. A method (method, see abstract line 1) for protecting sensitive information (call records, col. 3, line 38) in a network (local area network (LAN), col. 3 line 33), comprising: storing (abstract lines 4-5) the sensitive information at a network component (switch, abstract line 4); attaching a network device (adjunct processor (AP), abstract line 4, col.3 lines 2-3) to the network, the network device lacking the sensitive information and being inoperative, at least in part, until the sensitive information is stored therein; downloading (col. 3 line 39) the sensitive information from the network component to the network device; storing the sensitive information in the network device so that device becomes operational on the network; and when the device is disconnected from the network, erasing the sensitive information from the network device (According to hyperdictionary online: volatile storage is a computer storage that is erased when the

power is turned off. Therefore, it is factual in nature that if the power is disconnected from the device, the volatile memory (RAM) of the device would lose any data as soon as it is disconnected and the device will be non-operational).

Claim 15. A device (switch, abstract line 4) that is non-operational on a network (local area network (LAN), col. 3 line 33) unless the device is storing configuration information (stores call records, abstract, line 5) comprising: an interface (user interface, abstract line 3) for communication with the network; a memory (memory, abstract line 5) whose contents are erased upon loss of power to the device; and means for downloading (col. 3 line 39) from the network and storing in the memory the configuration information, wherein the configuration information, when stored in the memory, permits the device to operate on the network (According to hyperdictionary online: volatile storage is a computer storage that is erased when the power is turned off. Therefore, it is factual in nature that if the power is disconnected from the device, the volatile memory (RAM) of the device would lose any data as soon as it is disconnected and the device will be non-operational).

7. **Claims 22-24, 29, 34** are rejected under 35 U.S.C. 102(b) as being anticipated by Ryu (US 2001/0046224 dated 11/29/2001).

Claim 22. A network system (A system (radio data communication system, abstract line 1)), comprising: switch (LAN switch, abstract line 2) for attaching a device (Ethernet interface, [0038] line 1) and the network (IP network, abstract lines 2-3) so that information (program, [0041] lines 12-13) can be communicated between the device and the network system, wherein the device is not fully operational when first connected to the switch; and means for downloading configuration information from the network

system to a volatile memory (dynamic memory, [0037] lines 11-12, Fig. 3) included in the device in response to a request (This is inherent in nature as in order to download information, a request has to be made by the program, in order for the downloading to take place) from the device, the device being operable on the network after the configuration information is downloaded into the volatile memory (According to dictionary: volatile storage is a computer storage that is erased when the power is turned off. Therefore, it is factual in nature that if the power is disconnected from the device, the volatile memory (RAM or dynamic storage) of the device would lose any data as soon as it is disconnected and the device will be non-operational);

Claim 23. The network system (radio data communication system, abstract line 1) further comprises means for downloading an executable image (program, [0041] lines 12-13) from the network system to the device (LAN switch, abstract line 2).

Claim 24. The network system (radio data communication system, abstract line 1), wherein the request is generated by running the executable image (program, [0041] lines 12-13) on the device (LAN switch, abstract line 2)(This is inherent in nature as in order to download information, a request has to be made by the program, in order for the downloading to take place).

Claim 29. A system (radio data communication system, abstract line 1), comprising: a device (LAN switch, abstract line 2) including a network interface (Ethernet interface, [0038] line 1), a memory (dynamic memory, [0037] lines 11-12, Fig. 3) whose contents are erased upon loss of power to the device (This is factual as stated by the dictionary online as a storage, such as RAM, that loses all information when power is cut off), and a bootstrap program (booting, [0041] line 4) for downloading and storing an executable

image (program, [0041] lines 12-13) in the memory; and a network (IP network, abstract lines 2-3) including a port (Ethernet port, abstract line 19) for connecting to the network interface so that information can be communicated between the device and the network, wherein the device is fully operational when first connected to the port, and means for downloading the executable image from the network into the memory in response to a request from the bootstrap program (This is inherent in nature as in order to download information, a request has to be made by the program, in order for the downloading to take place), and means for downloading configuration information (This is factual in nature that data can be in the form of an image, program, key, picture, etc.) from the network to the memory in response to a request generated by running from the executable image at the device (This is inherent in nature as in order for the information to be downloaded, a request has to be made by the program), the device being operational on the network after the configuration information is downloaded into the memory.

Claim 34. A method for operating a device (LAN switch, abstract line 2), on a network (IP network, abstract lines 2-3), comprising: attaching the device to the network so that information can be communicated between the device and the network; downloading an executable image (program, [0041] lines 12-13) from the network to the device; executing the downloaded executable image at the device to obtain configuration information from the network; and storing the configuration information in a volatile memory (dynamic memory, [0037] lines 11-12, Fig. 3) included in the device, the device being operable on the network after the configuration information is downloaded to the volatile memory, wherein the contents of the volatile memory are lost when the device is

de-powered (This is factual as stated by the dictionary online as a storage, such as RAM, that loses all information when power is cut off).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claims 2 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997) as applied to claim 1 above, and further in view of Tirabassi et al (US 6,400,925 dated 06/04/2002).

Beckmann teaches all the limitations of claims 2 and 9 except that the sensitive information is selected from a group consisting of configuring information, a software image, and a combination of the forgoing. The general concept of selecting the sensitive information from a group is well known in the art as illustrated by Tirabassi et al. which discloses storing the static images and configuration information into memory (col. 6 lines 4-6). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann to include the information selection from a group as taught by Tirabassi et al. in order to offer a larger variety of the types of data being transmitted.

10. **Claims 3 and 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997) and Tirabassi et al as applied to claim 2 above, and further in view of Sumner et al. (US 2003/0142641 dated 07/31/2003).

Beckmann and Tirabassi et al. teaches all the limitations of claims 3 and 10 except that the configuration information is selected from a group consisting of a password, a user ID, a network security key, and any combination of the forgoing. The general concept of selecting the configuration information from a group is well known in the art as illustrated by Sumner et al. which discloses a key, logon ID, password, and other appropriate information being conveyed through the WLAN ([0033] lines 7-10). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann and Tirabassi et al. to include the use of selection of configuration information from of a group as taught by Sumner et al. as an obvious information choice in order to select from a wide variety of the type of data to increase versatility.

11. **Claims 4 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997) as applied to claim 1 above, and further in view of Sumner et al. (US 2003/0142641 dated 07/31/2003).

Beckmann teaches all the limitations of claims 2 and 9 except that the network device includes a volatile memory for storing the sensitive information. The general concept of storing information in a volatile memory is well known in the art as illustrated by Sumner et al. which discloses storage medium being the volatile memory ([0073] lines 14-15). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann to include the use of a volatile memory as taught by Sumner et al. in order to increase efficiency of the system and to release resources.

12. **Claims 6,13,19-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997), and further in view of Sumner et al. (US 2003/0142641 dated 07/31/2003).

Beckmann teaches all the limitations of claims 6,13,19-21 except that the network device is a wireless access points through which the security information is accessed by the end user devices and authenticating the device on the network. The general concept of using a wireless access point to access secure information is well known in the art as illustrated by Sumner et al. which discloses an access point having access to a list of authorized wireless devices along with associated methods and authenticating information can ascertain the authority of the wireless device and users to access the network ([0024] lines 4-12 and Fig. 1). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann to include the use of an access point as taught by Sumner et al. in order to connect secure wireless networks with wireless communication devices.

13. **Claims 25-28,30-33,35-38** are rejected under 35 U.S.C. 103(a) as being unpatentable over Ryu (US 2001/0046224 dated 11/29/2001), and further in view of Sumner et al. (US 2003/0142641 dated 07/31/2003).

Ryu teaches all the limitations of claims 25-28,30-33,35-38 except that the network device is a wireless access points through which the security information is accessed by the end user devices and authenticating the device on the network. The general concept of using a wireless access point to access secure information is well known in the art as illustrated by Sumner et al. which discloses an access point having access to a list of authorized wireless devices along with associated methods and authenticating information can ascertain the authority of the wireless device and users to access the network ([0024] lines 4-12 and Fig. 1). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ryu to include the use of an

access point as taught by Sumner et al. in order to connect secure wireless networks with wireless communication devices.

14. **Claims 7 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997), and further in view of Sumner et al. (US 2003/0142641 dated 07/31/2003).

Beckmann teaches all the limitations of claims 7 and 14 except that the network component is located in a secure environment. The general concept of securing a network component in a network is well known in the art as illustrated by Sumner et al. which discloses an access point having access to a list of authorized wireless devices along with associated methods and authenticating information can ascertain the authority of the wireless device and users to access the network ([0024] lines 4-12 and Fig. 1).

Additional security measures, such as employing user authentication requiring individual certificates, are also conveyed to the responsible parties in the system of control point, access point, and wireless device [0033]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann to include the use of a secure network to secure the component as taught by Sumner et al. in order to make the system more secure.

15. **Claims 16-18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckmann (5,659,604 dated 08/19/1997), and further in view of Ryu (US 2001/0046224 dated 11/29/2001),

Beckmann teaches all the limitations of claims 16-18 except that a bootstrap program for downloading from the network an executable image, which permits the device to download the configuration information and stores the executable image in the

memory. The general concept of downloading information from the network and storing it on the memory is well known in the art as illustrated by Ryu which discloses the controller downloading the program from the call manager through the LAN switch and the Ethernet interface and stores the program in the dynamic memory ([0041] lines 10-16). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Beckmann to include the use of a downloading means to download information onto the memory as taught by Ryu in order to receive and transmit information over the network as an obvious communication technique.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Supriya Ahuja whose telephone number is 571-270-1588. The examiner can normally be reached on Monday - Thursday 7:30 -5:00; 2nd Friday 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-1808. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business

Art Unit: 2109

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

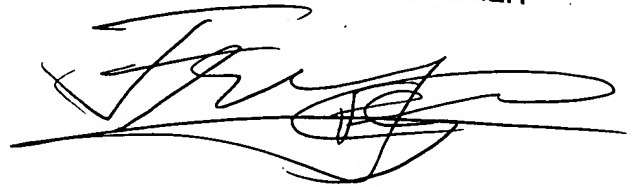
800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Supriya Ahuja

S.A.

January 18, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER

A handwritten signature in black ink, appearing to read 'Frantz', with a large, stylized flourish extending from the end of the signature.